

REMARKS

Claims 1-30 remain pending in the instant application. Claims 1-30 presently stand rejected. Reconsideration of the pending claims are respectfully requested.

Double Patenting Rejections – 35 U.S.C. § 101

Claims 1-30 stand provisionally rejected under 35 U.S.C. § 102(e) as being obvious over commonly assigned 10/462,996. Application 10/462,996 has been expressly abandoned as of (at least) August 16, 2007. (Also, see application 10/561,049, which formerly claimed priority to the now-abandoned application.) Because the application has been expressly abandoned, the rejections are moot.

Claim Rejections – 35 U.S.C. § 103

Claims 1-10, 13-19, 21-25, 27, 28, and 30 stand rejected under 35 U.S.C. § 102(e) as being obvious over IEEE's Port Based Network Access Control Protocol (802.1X-2001) in view of Intelligent Platform Management Interface (IPMI) Specification (version 1.5, revision 1.1, February 20, 2002).

Claim 1 recites:

1. A method comprising:
loading port authentication firmware instructions in a supplicant system;
and
authenticating a network port hosted by an authenticator system to which the supplicant system is linked via execution of the port authentication firmware instructions on the supplicant system.

In contrast, the combined references do not teach or suggest loading port authentication firmware instructions in a supplicant system. The office action concedes that the IEEE Port-Based Network Access Control protocol (IEEE) does not appear explicitly to disclose the loading port authentication firmware instructions in a supplicant system.

However, IPMI fails to overcome the deficiency of IEEE because the cited portion on 1.6.11 teaches support for storing and accessing... non-volatile information. The information referred to is inventory data such as serial number, part number, model,

and asset tag. There is no teaching or suggestion that the information be port authentication firmware instructions in a supplicant system. Figure 1-2 (IMPI Block Diagram) shows, for example, management busses communicating with FRU SEEPROMs. The diagram likewise does not show a teaching or suggestion that the information be port authentication firmware instructions in a supplicant system.

With respect to claim 15, claim 15 recites:

15. A method comprising:
executing instructions comprising port authentication code via a baseboard management controller (BMC) in a supplicant system to perform port authentication of a authenticator system port to which the supplicant system is linked in communication.

In contrast, the combined references do not teach or suggest executing instructions comprising port authentication code via a baseboard management controller (BMC) in a supplicant system. The office action concedes that the IEEE Port-Based Network Access Control protocol (IEEE) does not appear explicitly to disclose the executing instructions comprising port authentication code via a baseboard management controller (BMC) in a supplicant system.

However, IPMI fails to overcome the deficiency of IEEE because the cited portion (p. 23) discloses a BMC that is centrally positioned but does not teach or suggest executing instructions comprising port authentication code via a baseboard management controller (BMC) in a supplicant system.

With respect to claim 18, claim 18 recites:

18. A method comprising:
retrieving authentication credentials pertaining to a supplicant system during a pre-boot phase of the supplicant system;
passing the authentication credentials to an operating system running on the supplicant system during an operating system runtime phase; and

authenticating a network port to which the suppliant system is connected via use of the authentication credentials.

In contrast, the combined references do not teach or suggest retrieving authentication credentials pertaining to a suppliant system during a pre-boot phase of the suppliant system. The office action concedes that the IEEE Port-Based Network Access Control protocol (IEEE) does not appear explicitly to disclose retrieving authentication credentials pertaining to a suppliant system during a pre-boot phase of the suppliant system .

However, IPMI fails to overcome the deficiency of IEEE because the cited portion (p. 23) discloses remote authentication but does not teach or suggest retrieving authentication credentials pertaining to a suppliant system during a pre-boot phase of the suppliant system because section 36.2 (page 362) teaches sensor type codes that, for example, pass the result of a password violation, but does not pass the credentials themselves.

With respect to claim 25, claim 25 recites:

25. A suppliant system comprising:
a processor;
a network interface, coupled to the processor; and
a flash device coupled to the processor, having firmware instructions stored therein that when executed on the processor perform operations including:
authenticating a network port hosted by an authenticator system to which the suppliant system is linked in communication via the network interface.

In contrast, the combined references do not teach or suggest a flash device coupled to the processor having firmware instructions stored therein that when executed on the processor perform operations including authenticating a network port. The office action concedes that the IEEE Port-Based Network Access Control protocol (IEEE) does not appear explicitly to disclose a flash device coupled to the processor having firmware

instructions stored therein that when executed on the processor perform operations including authenticating a network port.

However, IPMI fails to overcome the deficiency of IEEE because the cited portions (pp. 162, 311, and 325) discloses flash memory as a place where data may be stored but does not teach or suggest a flash device coupled to the processor having firmware instructions stored therein that when executed on the processor perform operations including authenticating a network port. As discussed above with respect to claim 1, the disclosed data is not firmware instruction for, for example, authentication.

With respect to claim 28, claim 28 recites:

28. (Original) A supplicant system comprising:
- a baseboard management controller (BMC);
 - a network interface, coupled to the baseboard management controller; and
 - machine-executable instructions stored on the supplicant system, which when executed on the BMC perform operations including:
 - authenticating a network port hosted by an authenticator system to which the supplicant system is linked in communication via the network interface.

In contrast, the combined references do not teach or suggest machine-executable instructions stored on the supplicant system, which when executed on the BMC perform operations including authenticating a network port. The office action concedes that the IEEE Port-Based Network Access Control protocol (IEEE) does not appear explicitly to disclose machine-executable instructions stored on the supplicant system, which when executed on the BMC perform operations including authenticating a network port.

However, IPMI fails to overcome the deficiency of IEEE because the cited portions (as discussed with respect to claim 1) teaches support for storing and accessing... non-volatile information. The information referred to is inventory data such as serial number, part number, model, and asset tag. There is no teaching or suggestion that the information be port authentication firmware instructions in a supplicant system. Figure 1-2 (IMPI Block Diagram) shows, for example, management busses

communicating with FRU SEEPROMs. The diagram likewise does not show a teaching or suggestion that the information be port authentication firmware instructions in a supplicant system.

The office action further asserts that it would have been obvious to one of ordinary skill in the art, having the teachings of IEEE and the IPMI specification, to modify the authentication scheme of IEEE 802.1x to include storage of the authentication instructions in firmware, to execute these instructions during a pre-boot phase, and further to load an operating-system image over the network connection so authenticated.

The office action alleges the motivation for doing so would have been to take advantage of the behind-the-scenes feature (p. 13, first paragraph of IPMI) to streamline network authentication. The applicants traverse the alleged assertion and motivation because the motivation for the teaching to provide information access out-of-band or under system-down conditions to FRU or inventory data mechanisms, which are data, and not code. Thus the motivation to combine is not directed towards claim distinctions and fails to consider the invention as a whole.

The office action further alleges the motivation for doing so would be because the out-of-band password is (alleged) to be an indication that system administrators may put a measure of confidence in IPMI's design. With respect to data storage, the IPMI specification recommends the devices lacking integrity checks not be placed on "public" busses such as IPMB and PCI-SMBus because of possible data corruption. Thus the authors recognize that following the IPMI specification is inadequate for secure data storage.

The office action further alleges that enterprises have a vested interest in keeping up with current technology (such as ARP requests when the system is powered down or sleeping). Applicants traverse the statement as being too general as the alleged motivation would preclude patenting any improvement in current technology. There is no teaching or suggestion (other than in the applicants' own disclosure) to load port authentication firmware instructions in a supplicant system.

At least for the foregoing reasons, the combined references do not teach or suggest each and every element of the independent claims, therefore the independent claims and all claims which therefrom are patentable over the combination of references.

CONCLUSION

In view of the foregoing remarks, Applicants believe the applicable rejections have been overcome and all claims remaining in the application are presently in condition for allowance. Accordingly, favorable consideration and a Notice of Allowance are earnestly solicited. The Examiner is invited to telephone the undersigned representative at (206) 292-8600 if the Examiner believes that an interview might be useful for any reason.

CHARGE DEPOSIT ACCOUNT

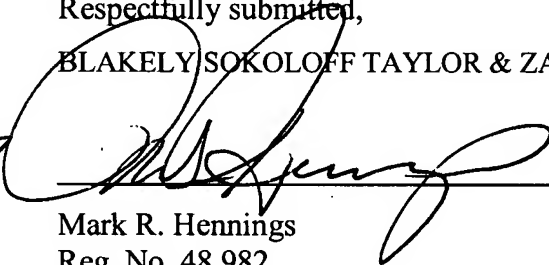
It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a). Any fees required therefore are hereby authorized to be charged to Deposit Account No. 02-2666. Please credit any overpayment to the same deposit account.

Respectfully submitted,

BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP

Date:

Sept 14, 2007


Mark R. Hennings
Reg. No. 48,982
Phone: (206) 292-8600

1279 Oakmead Parkway
Sunnyvale, California
94085-4040